
# bTrade TDAccess
# Technical Overview

Release 2.2

Document 2003.TO002.02
Printed in the USA.

# Contents

# 1 Introduction

For over 30 years, companies have been conducting business electronically. The exchanges were enabled by direct dial-up connections and private VANs[1]. Unfortunately, many small and medium enterprises were unable to use the technology—the benefits were always outweighed by the cost.

The Internet captured the attention of the business community a decade ago. Business analysts, even VAN operators, were announcing that this quickly maturing communications infrastructure would serve as the backbone for business-to-business exchanges. There was significant migration from VAN to the Internet exchanges; however, companies leveraging the technology were not the small or medium sized enterprises.

The Internet's benefits were not without risk. It was 'free', but could it be made secure or reliable? Almost immediately, Netscape© developed and fielded a technology for securing the communications channel. They contributed their work to the IETF[2], an international consortium focused on providing standard solutions for Internet activities, which published the work as a specification. This technology, commonly known as SSL[3], nullified many of the Internet security concerns. The IETF further aided business exchanges with publication of the EDIINT[4] specifications. The EDIINT work provided additional security mechanisms plus addressed the reliability issue. Two EDIINT solutions were produced. The AS1[5] solution provides secure messaging using electronic mail (SMTP[6]) and the AS2[7] solution provides similar services using HTTP[8].

Packaging of an affordable solution for small and medium enterprises was the last barrier. bTrade, Inc. conquered this obstacle with a versatile product that services enterprises regardless of size. Small companies with desktops and huge enterprises using mainframe computers are proving the utility of TDAccess™. Data transformation, compression, and communications services process structured and unstructured data with equal efficiency, and Internet-based communications channels can reach any enterprise on the planet.

# 2 TDAccess Overview

TDAccess is a complete communications solution supporting multiple data file formats, security protocols, and communication methods. It is designed to operate with a trading community administrator to define and manage trading relationships.

The utility of TDAccess is extended with the inclusion of an 'always-on' AS2 Server. The AS2 Server communicates between TDAccess and the other AS2 servers of the trading community. It not only receives and processes AS2-compliant messages but also processes MDNs[9] that are received in response to dispatched messages.

The TDAccess client performs all data formatting, compression, and security functions necessary to prepare messages. It also handles communications. It can send and receive messages over a variety of communication protocols. With the addition of the AS2 Server's receive functions, the world is now open for business.

## 2.1 TDAccess Client

TDAccess targets all business-to-business communications, regardless of the size of the enterprise. The software is currently available for a wide variety of platforms. Mainframe users on AS/400 or MVS systems will find that TDAccess performs as ruggedly as any other mainframe program. Those using UNIX systems will also discover that TDAccess integrates directly into their other processes. At present TDAccess is supported for HP-UNIX, AIX, and SUN-UNIX. Windows users are included as well. TDAccess operates on Windows 98, 2000, NT and XP. Linux is also supported. Regardless of computing environment, TDAccess is available.

TDAccess is designed to operate with other business applications. It may be executed three different ways: command line calls, library calls, or through a GUI[10]. Regardless of the business environment, the TDAccess client will support your secure data exchanges. The command line calls permit the TDAccess client to be launched from batch programs or job steps. The command line provides a broad set of parameters that tailor TDAccess operations. Users who want to call TDAccess client from within user-developed applications can use library calls provided with TDAccess. Finally, the GUI displays familiar buttons and dialogue boxes for defining stored or ad hoc transfers, as well as the other functions available to the command line and library interfaces. Note that GUI support is not available for AS/400 and MVS users.

TDAccess transforms the user's data into a variety of standard formats. Messages are constructed and secured based on configuration information provided through the TDManager runtime files. A central authority within a business community operates the TDManager. Security services applied to messages also comply with the security policy defined by the TDManager. While security configuration is handled by TDManager, TDAccess does permit users to request digital credentials from TDManager. TDAccess

functions allow users to generate key pairs[11] (protecting their private key) and to forward the public key to TDManager for incorporation into the user's digital certificate.

Data is transformed according to ANSI[12] and ISO[13] standards. When the user-requested security services are applied, TDAccess ensures that they are added according to published specifications—interoperable specifications. The software creates the special enveloping structures consistent with the ANSI ASC X12[14] or UN/EDIFACT[15] standards. Additionally, new data segments are automatically created and inserted into messages as required by the EDI standards. TDAccess supports the most popular versions of these standards. These include versions 3050 and 4010 of X12 and syntax 4 of EDIFACT. Support is also included for a special EDIFACT syntax version 3[16]. Of course, TDAccess supports unstructured data too. S/MIME encapsulation, used for AS1 and AS2 messages, and a proprietary encapsulation are both used to support messages containing unstructured data. This ensures that TDAccess messages can be sent to, or received from, trading partners not equipped with the TDAccess software.

File compression and filtering functions are also included in TDAccess. The compression algorithm, based on the widely used LZ77[17] compression algorithm can reduce the actual size of files by up to 85%. Compression can significantly reduce transfer times over the Internet. When files are being sent to external VANs, compression can greatly reduce the cost related to individual messages for the receiver. Regarding filtering, two filtering algorithms, HEX[18] and Base-64[19], are built into TDAccess. The filtering algorithms allow files to be safely communicated across networks that may not like binary data.

If trading partners can be reached via the Internet, TDAccess can communicate with them. Many trading partners support FTP[20] communications. TDAccess supports a variety of FTP connections. Bi-directional FTP exchanges are supported by a variety of FTP connection types. The TDAccess client not only supports standard FTP exchanges, but also privately defined FTP formats. Several of the FTP formats implement SSL for additional session-level security. A powerful bTrade-developed secure FTP format that provided SSL services is also include in TDAccess. This FTP capability can optionally merge the FTP commands and data on a single channel, as well as control the client-side Internet port addresses used to communicate. These options can overcome most firewall configuration issues. Processing support for AS1 is also provided. An embedded SMTP processor supports AS1 transfers. The SMTP processor forwards the AS1 message to an e-mail exchange. TDAccess users must provide a POP3[21] server—it is not a component within the TDAccess client. Finally, the TDAccess client creates and forwards AS2 compliant messages. Security services are applied, data are enveloped, and messages are forwarded over defined HTTP channels.

TDAccess supports a rich set of cryptographic tools. Strong encryption algorithms, used in financial and government transactions, are built into the software. Popular encryption algorithms like Triple DES[22] and RSA[23] are available on demand. Digital signing is created using the RSA signature technique. And, TDAccess includes lesser known, but

nonetheless important algorithms, such as RC2, NVB7[24] and ISO9796[25] padding for good measure. Now, authenticated messages can be exchanged with privacy guaranteed.

## 2.2 AS2 Server

The AS2 Server that is supplied with TDAccess is an 'always on' application that ensures that trading partners have constant access to you. The server perpetually listens for messages from other AS2 servers, servicing them immediately upon receipt.

The AS2 Server is interoperable with any other certified AS2 server. It has been certified as compliant with the IETF AS2 specification through independent, interoperability testing. Our server uses the same runtime files as TDAccess to provide message services. The design ensures tight integration between the two products.

In response to received messages, the AS2 Server can automatically generate MDN. The specific content of the MDN varies based on an interrogation of the message by the AS2 Server. If the message originator requests a receipt, the AS2 Server acknowledges receipt of the message and the status of the security services associated with the message. Messages that contain valid, verifiable information are acknowledged as successfully received. When errors are detected, the MDN reports the nature of the error. All MDN can be signed to verify the sender's identity.

The AS2 Server supports both synchronous and asynchronous communications sessions. HTTP transfers are specified for AS2 messages. The AS2 Server can return the MDN in the same communications session that delivered the message. In these cases, the MDN is returned with the standard HTTP status message. The AS2 Server can also transmit the MDN in a separate communications session. When asynchronous responses are requested, the AS2 Server can use HTTP or SMTP to deliver the MDN. The AS2 Server offers full HTTP proxy support when sending asynchronous MDN.

TDAccess may configure a database to audit MDN activity. If the database is present, all MDN activity is recorded in the database. This database allows the TDAccess user to apply strict discipline to their communication processes.

## 2.3 TDAccess Configuration

The TDAccess programs are delivered on a CD-ROM and require configuration before they can be used. Software installation is completed using an automated installation process. When the installation process completes, programs and their associated files are correctly located on the system; however, the programs do not have sufficient information to function.

TDAccess users must complete several configuration steps. The most significant is that runtime files must be obtained and installed. The runtime file contains digital certificates

and security policy information related to the TDAccess user. Digital certificates for not only the TDAccess owner but also all the trading partners associated with the owner are contained in the runtime file. This file also defines what types of data are being exchanged and what security services are required for the exchanges. This file must be obtained from the TDManager associated with your business community.

If the TDAccess user intends to exchange AS2-compliant messages, the AS2 Server configuration file must be updated. This is a straightforward task, easily completed by individuals capable of using standard text editors.

The MDN database is also optional, but must be configured before use. The MDN database maintains an audit of MDN activity for AS1 and AS2 exchanges. An individual knowledgeable of database administration will be required to initialize the MDN database, but the actual tasks required are elementary.

This process has been simplified by detailed installation instructions and the availability of highly skilled technical support personnel. While the list looks rather daunting, there are only a few entries required in the configuration and initialization files.

The configuration process is greatly simplified for TDAccess owners who elect to acquire their software directly through the bTrade, Inc. website. A series of web pages gather the information required to pre-configure the software and deliver the information with the TDAccess software during the download. Not all information is collected during this process; however, users will discover that the vast majority of the configuration is already done when the software is downloaded to their site. Click a button and the software is downloaded. An installation wizard leads the TDAccess owner through the installation process. Make a couple additions to personalize the application and the configuration is complete. The process is designed to have the TDAccess software supporting the customer's business processes as quickly as possible.

# 3 References

## 3.1 Glossary

An extensive and update-to-date glossary is maintained on the bTrade website at: http://www.btrade.com/G0.htm.

## 3.2 Document Footnotes

1 Value-Added Network.
2 Internet Engineering Task Force. The Internet Engineering Task Force (IETF) is a large open international community of individuals concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
3 Secure Sockets Layer. Since replaced by the Transport Layer Security (TLS) standard, the Secure Sockets Layer (SSL) remains a commonly used protocol for managing the security of a message transmission on the Internet.
4 EDI Over-the-Internet. The initial IETF RFC1767 defined the method for packaging the EDI X12 and UN/EDIFACT transactions sets in a MIME envelope.
[5]5 Application Statement 1. This is an Internet solution for securely exchanging EDI over the Internet. This document expands on RFC 1767 to specify use of a comprehensive set of data security features, specifically data privacy, data integrity/authenticity, non-repudiation of origin and non-repudiation of receipt. This technique relies on using electronic mail as the technique for delivering the messages.
6 Simple Mail Transfer Protocol. This is an IETF specification defining the method for exchanging electronic mail over the Internet.
7 Application Statement 2. It builds on the AS1 work. The goal is to make use of HTTP instead of SMTP as a transport protocol, and make the changes that are needed to adapt to protocol packaging differences. This technique uses the Hypertext Transfer Protocol to transport the messages.
8 Hypertext Transfer Protocol. The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
9 Message Disposition Notification messages. These messages are designed to report the status of AS2 messages exchanged between AS2 servers. The messages report the satisfactory receipt and errors.
10 Graphical User Interface. A GUI (usually pronounced GOO-ee) is a graphical (rather than purely textual) user interface to a computer.
[11] Public-private key pairs are basic components of a Public Key Infrastructure. The keys are a matched set. The private key is protected by the owner of the key pair while the public portion is published for use by everyone requiring it.
[12] American National Standards Institute.
[13] International Standards Organization.
[14] American National Standards Institute Accredited Subcommittee X12 is responsible for the development and maintenance of the EDI syntax for North America. BTrade, Inc is an active member in this group. Currently, the Vice Chair of the organization is from bTrade, Inc.
[15] United Nations/ Electronic Data Interchange For Administration, Commerce, and Transport. This is the UN implementation of the EDIFACT syntax. Originally, specified and maintained by a work group within the UN, the syntax is now defined through a joint UN/ISO committee. The syntax is defined in ISO Standard 9735. bTrade, Inc. supported the development of the security components of this standard. The convener of the security syntax group is from bTrade, Inc.
[16] The UN/CEFACT EDIFACT Work Group, Finance Committee (D6), produced a proposed syntax 3 implementation that supported basic security needs. The proposed solution is in wide use within the European banking community.

[17] Lempel Ziv 77. In 1977, Abraham Lempel and Jacob Ziv presented their dictionary-based scheme for text compression, the scheme was called LZ77.
18 Hexadecimal filtering. Hexadecimal describes a base-16 number system. That is, it describes a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. The hexadecimal numbers are 0-9 and then use the letters A-F.
19 Base 64 Filtering. This is a popular filtering method used in Internet applications. It converts binary streams into one of a set of 64 character values that are friendly to networks.
20 File Transfer Protocol.
21 Post Office Protocol 3. Post Office Protocol 3 (POP3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server.
22 Triple Data Encryption Standard (DES3) is a derivative of the ubiquitous Data Encryption Standard (DES) that has served as the cornerstone of data encryption for almost 40 years. The technique employs three iterations of the DES algorithm in a well-specified encrypt-decrypt-encrypt methodology.
23 RSA. RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browser from Netscape and Microsoft. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key.
24 A hashing and signing algorithm used by Norwegian banking entities.
25 TDAccess supports version 1 and 2 of ISO 9796. Both standards address mechanisms for padding a hash value. Version 1 was withdrawn as an ISO standard due to perceived security vulnerability. Nevertheless, many companies continue to use version 1 so the product includes this support.